Traductions Bien Fait Translations
Done Well ... Done Right

December 18, 2009

Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

Commissioner for Patents,

I, Bruce D. Popp, undersigned, am a professional translator fluent in French and English. I am American Translators Association Certified for translation from French into English.

I state that to the best of my knowledge and belief I have accurately translated into English the French document, PCT application WO95/28058 page 3, line 23 through page 7, line 3 and that I am attaching said accurate translation.

I affirm that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true.

I am aware that willful false statements and the like are punishable by fine or imprisonment, or both (Title 18 United States Code section 1001) and may jeopardize the validity of the application or any patent issuing thereon.

Bruce D. Popp

ATA Certified Translator
Bruce D. Popp, Ph.D.
Patent Translation Specialist
Bien Fait Translations
+1 508-624-9767
French into English

50 BRIARWOOD LANE, APT. 5 • MARLBOROUGH, MA 01752, • UNITED STATES
PHONE: 866-243-6324
BDPOPP@BIEN-FAIT.COM

Description of the Invention

The present invention therefore covers especially a specific step from the broadcast process for progressive conditional access programs, specifically the step of preparing the two flows referred to as elementary and complementary. The invention applies in the case where the information flow leaving the coder is digital, because this is the case in which the most difficult problems for progressive conditional access occur. Further, it is assumed that the information is multiplexed, meaning that they made up of a "multiplex" formed from a series of elements which can be, depending on the type of the multiplexing: frames, packets, etc.

Under these conditions, and according to the invention, to separate the multiplexed information flow into a basic flow and complementary flow, groups of *m* successive elements and *p* successive elements from the multiplex are taken alternately, where the groups of *m* elements constitute the elementary flow and the groups of *p* elements the complementary flow.

Specifically, the purpose of the present invention is a broadcast process for progressive conditional access programs, in which:

- An information flow corresponding to a program component is separated into a first flow, referred to as elementary flow, and into a second flow, referred to as complementary flow;
- At least the complementary flow is scrambled using a control word;
- Synchronously with each program, access control messages are transmitted making it possible to descramble and restore the scrambled flows in receivers having the corresponding access rights; restitution of only the elementary flows leads to a discernible program component without being directly usable; descrambling of the complementary flow makes it possible to complete the program component in order to enable the complete restitution of the program;

since this process is characterized by the fact that—the information flow being in digital multiplex constituted of a series of elements—the elementary flow is constituted by taking groups of *m* successive elements in the multiplex and the complementary flow is constituted by taking groups of *p* successive elements in the multiplex, where the groups of *m* successive

elements alternate with the groups of *p* successive elements.

In a first embodiment, the elements of the multiplex are fixed length frames, broken down into variable length channels, where the program component to be scrambled is transmitted in a channel whose row is predetermined; the elementary flow is constituted by taking the information contained in a channel with predetermined row *i* in the groups of *m* successive frames and the complementary flow is constituted by the information contained in the channel with the same predetermined row *i* in the groups of *p* successive frames alternating with said groups of *m* successive frames.

In a first variant, the channel with predetermined row *i* from the groups of the *m* successive frames is scrambled with the first control word CW1 and the channel with same row *i* from the groups of *p* successive frames is scrambled by a second control word CW2.

The control word CW1 could be the known local control word from the receiver or a control word carried inside an access control message.

In another variant, the channel from predetermined row *i* from the groups of *m* successive frames is not scrambled, but the channel from predetermined row *i* from the groups of *p* successive frames is scrambled with the control word (CW2).

In a second embodiment, the elements of the multiplex are packets and the elementary flux is constituted by the information contained in groups of *m* successive packets and the complementary flow is constituted by the information contained in the

groups of *p* successive packets alternating with the groups of *m* successive packets.

In a first variant, the packets from the groups of *m* successive packets are scrambled by a first control word CW1 and the groups of *p* successive packets by a second control word CW2.

In a second variant, the packets from the groups of *m* successive packets are not scrambled but the groups of *p* successive packets are scrambled by a control word (CW2).

An object of the present invention is also a receiver suitable for receiving the programs broadcast according to the process which was just defined. This receiver is characterized by the fact that it comprises:

- Means for separating in the received information flow a first flow, referred to as elementary flow, constituted by groups of *m* successive elements, and a second flow, referred to as complementary flow, constituted by groups of *p* successive elements, where the groups of *m* successive elements alternate with the groups of *p* successive elements;
- Means for recognizing at least one access control message in the received information and extracting at least one control word and at least one access condition;
- Means for verifying whether said access condition is satisfied;
- Means for descrambling at least the complementary flow by using the associated control word if the corresponding access condition is satisfied;
- At least one video, audio or data receiver receiving at least the elementary flow signals

and, when applicable, the de-scrambled complementary flow signals if the corresponding access condition is satisfied.


(WO/1995/028058) METHOD FOR BROADCASTING GRADUAL CONDITIONAL ACCESS PROGRAMMES WITH DATA FLOW SEPARATION, AND RECEIVER THEREFOR

Biblio. Data | Description | Claims | National Phase | Notices | Documents

Latest bibliographic data on file with the International Bureau

Pub. No.: WO/1995/028058
Publication Date: 19.10.1995
International Application No.: PCT/FR1995/000435
International Filing Date: 05.04.1995
Chapter 2 Demand Filed: 18.10.1995

IPC: ***H04N 7/167*** (2006.01)

Applicants: **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).
TELEDIFFUSION DE FRANCE [FR/FR]; 10, rue d'Oradour-sur-Glane, F-75015 Paris (FR).

Inventors: **GIACHETTI, Jean-Luc**; (FR).
GUILLOU, Louis; (FR).
PACAUD, Jean-Claude; (FR).

Agent: **BREVATOME**; 25, rue de Ponthieu, F-75008 Paris (FR).

Priority Data: 94/04012 06.04.1994 FR

Title: (EN) METHOD FOR BROADCASTING GRADUAL CONDITIONAL ACCESS PROGRAMMES WITH DATA FLOW SEPARATION, AND RECEIVER THEREFOR

(FR) PROCEDE DE DIFFUSION DE PROGRAMMES A ACCES CONDITIONNEL PROGRESSIF ET A SEPARATION DU FLUX D'INFORMATION ET RECEPTEUR CORRESPONDANT

Abstract: (EN) A method for broadcasting gradual conditional access programmes with data flow separation, and a receiver therefor. A basic flow is formed by providing groups of m successive multiplex elements and a complementary flow is formed by providing groups of p successive multiplex elements. The method is useful in pay television.

(FR) Pour constituer le flux élémentaire, on prend des groupes de m éléments successifs du multiplex et pour constituer le flux complémentaire, on prend des groupes de p éléments successifs du multiplex. Application à la télévision à contrôle d'accès.

Designated States: CA, JP, KR, NO.
European Patent Office (EPO) (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publication Language: French (FR)

Filing Language: French (FR)

PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 : H04N 7/167 — A1

(11) Numéro de publication internationale: WO 95/28058

(43) Date de publication internationale: 19 octobre 1995 (19.10.95)

(21) Numéro de la demande internationale: PCT/FR95/00435

(22) Date de dépôt international: 5 avril 1995 (05.04.95)

(30) Données relatives à la priorité:
94/04012 6 avril 1994 (06.04.94) FR

(71) Déposants: FRANCE TELECOM [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR). TELEDIFFUSION DE FRANCE [FR/FR]; 10, rue d'Oradour-sur-Glane, F-75015 Paris (FR).

(72) Inventeurs: GIACHETTI, Jean-Luc; 10, rue Paul-Gauguin, F-35830 Betton (FR). GUILLOU, Louis; 16, rue de l'Ise, F-35230 Bourgbarre (FR). PACAUD, Jean-Claude; 14, rue de l'Epinette, F-35260 Cancale (FR).

(74) Mandataire: BREVATOME; 25, rue de Ponthieu, F-75008 Paris (FR).

(81) Etats désignés: CA, JP, KR, NO, brevet européen (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.

(54) Title: METHOD FOR BROADCASTING GRADUAL CONDITIONAL ACCESS PROGRAMMES WITH DATA FLOW SEPARATION, AND RECEIVER THEREFOR

(54) Titre: PROCEDE DE DIFFUSION DE PROGRAMMES A ACCES CONDITIONNEL PROGRESSIF ET A SEPARATION DU FLUX D'INFORMATION ET RECEPTEUR CORRESPONDANT

(57) Abstract

A method for broadcasting gradual conditional access programmes with data flow separation, and a receiver therefor. A basic flow is formed by providing groups of m successive multiplex elements and a complementary flow is formed by providing groups of p successive multiplex elements. The method is useful in pay television.

(57) Abrégé

Pour constituer le flux élémentaire, on prend des groupes de m éléments successifs du multiplex et pour constituer le flux complémentaire, on prend des groupes de p éléments successifs du multiplex. Application à la télévision à contrôle d'accès.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AT	Autriche	GB	Royaume-Uni	MR	Mauritanie
AU	Australie	GE	Géorgie	MW	Malawi
BB	Barbade	GN	Guinée	NE	Niger
BE	Belgique	GR	Grèce	NL	Pays-Bas
BF	Burkina Faso	HU	Hongrie	NO	Norvège
BG	Bulgarie	IE	Irlande	NZ	Nouvelle-Zélande
BJ	Bénin	IT	Italie	PL	Pologne
BR	Brésil	JP	Japon	PT	Portugal
BY	Bélarus	KE	Kenya	RO	Roumanie
CA	Canada	KG	Kirghizistan	RU	Fédération de Russie
CF	République centrafricaine	KP	République populaire démocratique de Corée	SD	Soudan
CG	Congo			SE	Suède
CH	Suisse	KR	République de Corée	SI	Slovénie
CI	Côte d'Ivoire	KZ	Kazakhstan	SK	Slovaquie
CM	Cameroun	LI	Liechtenstein	SN	Sénégal
CN	Chine	LK	Sri Lanka	TD	Tchad
CS	Tchécoslovaquie	LU	Luxembourg	TG	Togo
CZ	République tchèque	LV	Lettonie	TJ	Tadjikistan
DE	Allemagne	MC	Monaco	TT	Trinité-et-Tobago
DK	Danemark	MD	République de Moldova	UA	Ukraine
ES	Espagne	MG	Madagascar	US	Etats-Unis d'Amérique
FI	Finlande	ML	Mali	UZ	Ouzbékistan
FR	France	MN	Mongolie	VN	Viet Nam
GA	Gabon				

PROCEDE DE DIFFUSION DE PROGRAMMES A ACCES CONDITIONNEL PROGRESSIF ET A SEPARATION DU FLUX D'INFORMATION ET RECEPTEUR CORRESPONDANT

Domaine technique

La présente invention a pour objet un procédé de diffusion de programmes à accès progressif et à séparation du flux d'information et un récepteur correspondant.

Elle trouve une application dans la télévision à péage, dans la diffusion de programmes radiophoniques ou de sons ou de données, dans la transmission et la distribution d'éléments de programmes, etc...

Etat de la technique antérieure

Dans les systèmes classiques de diffusion de programmes, l'accès aux programmes est réservé à une certaine population de récepteurs. S'il est possible de distinguer divers droits d'accès (un programme peut être par exemple simultanément accessible par abonnement et par achat impulsif), il demeure qu'un récepteur est ou n'est pas autorisé selon qu'il dispose ou non d'un certain droit d'accès.

Or, pouvoir attirer le télespectateur ou l'auditeur en découvrant volontairement tout ou partie du contenu de l'image ou du son d'un programme pendant une période de temps donnée est un atout commercial important pour tout système d'accès conditionnel. Cette fonction existe actuellement sur certains systèmes de télévision à péage utilisant un procédé d'embrouillage ne transformant pas profondément l'image. Mais en numérique, les techniques d'embrouillage couramment utilisées transforment trop profondément le signal pour

permettre de laisser "deviner" le programme à l'utilisateur.

La demande de brevet français n°92 15841 déposée le 29 décembre 1992 et intitulée "Procédé de diffusion de programmes à accès conditionnel permettant un accès progressif à de tels programmes" ou la demande américaine correspondante 08/172,817 du 27 décembre 1993 décrit une technique permettant d'avoir un "aperçu" de certains programmes. Cet aperçu est rendu possible par l'usage d'un droit d'accès qui n'est que partiel, au contraire du droit d'accès habituel, qui est total. Ainsi, à côté des récepteurs autorisés, qui peuvent accéder complétement à un programme et des récepteurs non autorisés, qui ne peuvent rien recevoir de celui-ci, on trouve, selon cette technique, d'autres récepteurs pouvant avoir un aperçu du programme, c'est-à-dire pouvant accéder à une forme discernable mais non utilisable du programme.

Le procédé décrit dans cette demande de brevet comprend les opérations suivantes :

- on embrouille des informations propres à divers programmes,
- on transmet les informations ainsi embrouillées pour chaque programme,
- de manière synchronisée avec chaque programme, on transmet des messages de contrôle d'accès propres à chacun de ces programmes, ces messages étant aptes à permettre le désembrouillage et la restitution des programmes dans des récepteurs disposant des droits d'accès correspondant,
- on transmet en outre des messages de contrôle d'accès partiel à au moins certains de ces programmes, ces messages de contrôle d'accès partiel étant aptes à permettre le

désembrouillage et la restitution partielle des programmes correspondants pour des récepteurs disposant d'un droit d'accès partiel.

De manière avantageuse, pour mettre en oeuvre ce procédé, on découpe le flux d'information correspondant à chaque programme en un premier flux dit flux élémentaire, correspondant à un programme qui, une fois restitué dans un récepteur, sera discernable sans être directement utilisable, et un second flux, dit flux complémentaire, permettant de compléter le premier, pour permettre de restituer complétement le programme.

Dans cette variante, les messages de contrôle d'accès partiel s'appliquent aux flux élémentaires.

Le problème technique que se propose de résoudre la présente invention est la production du flux élémentaire et du flux complémentaire que nécessite cette technique et cela à partir d'un flux unique sortant d'un codeur quelconque.

Exposé de l'invention

La présente invention porte donc, notamment, sur une étape particulière du procédé d'émission de programmes à accès conditionnel progressif, à savoir l'étape de formation des deux flux dits élémentaire et complémentaire. L'invention s'applique dans le cas où le flux d'information sortant du codeur est de type numérique, car c'est dans ce cas que se posent les problèmes les plus ardus pour l'accès conditionnel progressif. Par ailleurs, on suppose que les informations sont multiplexées, c'est-à-dire qu'elles constituent un "multiplex" formé d'une suite d'éléments qui peuvent être, selon la nature du multiplexage, des trames, des paquets, ou autres, ...

Dans ces conditions et selon l'invention, pour séparer le flux d'information multiplexé en un flux élémentaire et en un flux complémentaire, on prend alternativement des groupes de m éléments successifs et de p éléments successifs du multiplex, les groupes de m éléments constituant le flux élémentaire et les groupes de p éléments le flux complémentaire.

De façon précise, la présente invention a donc pour objet un procédé de diffusion de programmes à accès conditionnel progressif, dans lequel :

- on sépare un flux d'information corespondant à une composante d'un programme en un premier flux, dit flux élémentaire et en un second flux, dit flux complémentaire,
- on embrouille au moins le flux complémentaire à l'aide d'un mot de contrôle,
- de manière synchrone avec chaque programme, on transmet des messages de contrôle d'accès permettant de désembrouiller et de restituer les flux embrouillés dans des récepteurs disposant des droits d'accès correspondants, la restitution du seul flux élémentaire conduisant à une composante de programme discernable sans être directement utilisable, le désembrouillage du flux complémentaire permettant de compléter la composante du programme pour permettre de restituer complétement le programme,

ce procédé étant caractérisé par le fait que, le flux d'information étant sous forme de multiplex numérique constitués d'une suite d'éléments, on constitue le flux élémentaire en prenant, dans le multiplex, des groupes de m éléments successifs et on constitue le flux complémentaire en prenant, dans le multiplex, des groupes de p éléments successifs, les groupes de m

éléments successifs alternant avec les groupes de p éléments successifs.

Dans un premier mode de mise en oeuvre, les éléments du multiplex sont des trames de longueur fixe, découpées en canaux de longueur variable, la composante du programme à embrouiller étant transmise dans un canal de rang déterminé ; on constitue alors le flux élémentaire en prenant les informations contenues dans un canal de rang déterminé i dans les groupes de m trames successives et le flux complémentaire par les informations contenues dans le canal de même rang déterminé i dans des groupes de p trames successives alternant avec lesdits groupes de m trames successives.

Dans une première variante, on embrouille le canal de rang déterminé i des groupes de m trames successives par un premier mot de contrôle CW1 et le canal de même rang i des groupes de p trames successives par un second mot de contrôle CW2.

Le mot de contrôle CW1 peut être le mot de contrôle local connu du récepteur ou un mot de contrôle véhiculé à l'intérieur d'un message de contrôle d'accès.

Dans une autre variante, on n'embrouille pas le canal de rang déterminé i des groupes de m trames successives mais on embrouille le canal de rang déterminé i des groupes de p trames successives par un mot de contrôle (CW2).

Dans un second mode de mise en oeuvre, les éléments du multiplex sont des paquets et on constitue le flux élémentaire par les informations contenues dans des groupes de m paquets successifs et le flux complémentaire par les informations contenues dans des

groupes de p paquets successifs alternant avec les groupes de m paquets successifs.

Dans une première variante, on embrouille les paquets des groupes de m paquets successifs par un premier mot de contrôle CW1 et les paquets des groupes de p paquets successifs par un second mot de contrôle CW2.

Dans une seconde variante, on n'embrouille pas les paquets des groupes de m paquets successifs, mais on embrouille les paquets des groupes de p paquets successifs par un mot de contrôle (CW2).

La présente invention a également pour objet un récepteur apte à recevoir les programmes émis selon le procédé qui vient d'être défini. Ce récepteur est caractérisé par le fait qu'il comprend :

- des moyens pour séparer dans le flux d'information reçu un premier flux, dit flux élémentaire, constitué par des groupes de m éléments successifs, et un second flux, dit flux complémentaire, constitué par des groupes de p éléments successifs, les groupes de m éléments successifs alternant avec les groupes de p éléments successifs,
- des moyens pour reconnaître au moins un message de contrôle d'accès dans les informations reçues et pour en extraire au moins un mot de contrôle et au moins une condition d'accès,
- des moyens pour vérifier si au moins ladite condition d'accès est satisfaite,
- des moyens pour désembrouiller au moins le flux complémentaire à l'aide du mot de contrôle associé si la condition d'accès correspondante est satisfaite,
- au moins un récepteur vidéo, audio ou de données recevant au moins les signaux du flux élémentaire

et, le cas échéant, les signaux du flux complémentaire désembrouillé si la condition d'accès correspondante est satisfaite.

Brève description des dessins

- la figure 1 est un diagramme schématique montrant une chaîne de diffusion de télévision à péage ;
- la figure 2 est un schéma montrant l'organisation d'un multiplex conforme à la technique de multiplexage en trames ;
- la figure 3 est un schéma montrant l'organisation d'un multiplex conforme à la technique de multiplexage en paquets ;
- la figure 4 illustre la constitution du flux élémentaire et du flux complémentaire dans le cas d'un multiplex en trames ;
- la figure 5 montre des composantes respectivement embrouillée, dégradée et désembrouillée dans le cas précédent ;
- la figure 6 illustre les moyens permettant de mettre en oeuvre le procédé de l'invention dans le cas du multiplexage en trames ;
- la figure 7 illustre la constitution du flux élémentaire et du flux complémentaire dans le cas d'un multiplex en paquets ;
- la figure 8 montre les composantes respectivement embrouillée, dégradée et désembrouillée dans le cas précédent ;
- la figure 9 illustre les moyens permettant de mettre en oeuvre le procédé de l'invention dans le cas du multiplexage en paquets ;
- la figure 10 montre le schéma synoptique d'un récepteur apte à traiter les signaux diffusés selon le procédé de l'invention ;

- la figure 11 illustre le fonctionnement du démultiplexeur-désembrouilleur dans le cas d'un multiplex tramé ;
- la figure 12 illustre le fonctionnement du démultiplexeur-désembrouilleur dans le cas d'un multiplex en paquets.

Exposé détaillé de modes de réalisation de l'invention

La figure 1 montre une chaîne classique de diffusion de programmes de télévision à péage. Cette chaîne comprend, côté émission, des codeurs source, en l'espèce deux codeurs référencés 10 et 10', un multiplexeur/embrouilleur 12, et, côté réception, un démultiplexeur/désembrouilleur 14 et des décodeurs source, en l'espèce deux décodeurs référencés 18 et 18'.

Les flux d'information issus des codeurs source 10 et 10' alimentent le multiplexeur/embrouilleur 12, qui est chargé de multiplexer et d'embrouiller ces flux afin de délivrer un flux unique qui est le flux diffusé.

L'embrouillage est une opération réversible visant à transformer le signal émis à l'aide d'une clé appelée mot de contrôle (CW), afin de rendre ce programme inintelligible pour les usagers ne possédant pas ce mot de contrôle.

Afin de permettre le désembrouillage , le mot de contrôle est transmis sous forme chiffrée dans des messages de contrôle d'accès appelés ECM. Chaque ECM contient également la condition d'accès (CA) devant être satisfaite par le module de contrôle d'accès de l'usager pour permettre le déchiffrement du mot de contrôle (CW) et, par conséquent, le désembrouillage du signal.

Les mots de contrôle ont une durée de vie limitée (typiquement 10 secondes). Afin d'éviter tout problème lors des changements de mot de contrôle, les deux mots de contrôle respectivement courant et futur sont transmis dans le message de contrôle d'accès. L'un est le mot de contrôle pair utilisé pendant une phase paire et noté CW_e ; l'autre est le mot de contrôle impair noté CW_o utilisé pendant une phase impaire.

Les flux d'information issus des codeurs source sont multiplexés temporellement. Deux techniques sont principalement utilisées dans le domaine de la diffusion numérique, le multiplexage en trame et le multiplexage en paquets.

Dans le multiplexage en trames, le multiplex est constitué d'une succession de trames de longueur fixe ayant toutes la même organisation, comme indiqué sur le schéma de la figure 2 qui montre une trame de rang i et la trame suivante de rang i+1.

Une trame est découpée en n canaux de longueur variable. Chaque canal véhicule un flux élémentaire (vidéo, son, ...). La même découpe est utilisée pour toutes les trames (des reconfigurations de multiplex sont possibles mais rares). Le débit alloué à un canal de rang k est égal à (Lgk)/Tbits/s, où Lgk est la longueur du canal k en bits et T la période de la trame.

A titre d'exemple, on peut citer le multiplex STERNE qui est un multiplex tramé. La longueur d'une trame est de 24ms. Le débit alloué à un canal qui aurait une longueur de 1 octet serait environ égal à 333 bits/s.

En général, un canal est réservé pour véhiculer une voie de service décrivant tous les autres canaux de la trame : longueur du canal, description du flux

élémentaire transporté dans le canal, paramètres d'embrouillage et de contrôle d'accès, ...

La voie de service transporte également un compteur de trames utilisé par exemple pour fixer la durée de vie des mots de contrôle ainsi que la parité de la phase.

L'embrouillage d'un flux élémentaire se fait actuellement en embrouillant, dans toutes les trames, tous les bits du canal véhiculant le flux élémentaire. Sur la figure 2, l'embrouillage porte sur le canal 2 et il est symbolisé par les hachures.

Quant au multiplexage en paquets, il consiste à produire une succession de paquets de longueur fixe ou variable. Chaque paquet contient les données d'un flux élémentaire. Le schéma de la figure 3 donne un exemple de multiplex en paquets, véhiculant trois flux élémentaires A, B et C.

Chaque paquet est constitué d'un en-tête (E-T), d'un champ de données et d'un suffixe (Sfx).

L'embrouillage d'un flux élémentaire se fait actuellement en embrouillant tous les champs de données des paquets véhiculant ce flux élémentaire. Dans l'exemple illustré sur la figure 3, seul le flux élémentaire B est embrouillé (les hachures symbolisent l'embrouillage).

A titre d'exemple, le multiplex MPEG2 est un multiplex par paquets dans lequel les paquets ont tous une longueur fixe de 188 octets. L'en-tête contient un identifiant du flux élémentaire, plus deux bits précisant le mode et les paramètres d'embrouillage utilisés pour ce paquet. Les valeurs de ces deux bits sont actuellement normalisées :

00 : pas d'embrouillage

01 : réservé

10 : embrouillage avec le mot de contrôle pair
11 : embrouillage avec le mot de contrôle impair.

Dans la demande de brevet n°92 15841 (US 08/172,817)déjà citée, il est décrit comment mettre en oeuvre un mécanisme d'embrouillage progressif dans le cas où la composante (vidéo ou audio) se présente en deux flux discernables. Il suffit, dans ce cas, d'appliquer un mot de contrôle CW1 (associé à une condition d'accès CA1) au flux élémentaire et un mot de contrôle CW2 (associé à une condition d'accès CA2) au flux complémentaire. La condition d'accès CA1 et le cryptogramme de CW1 sont transportés dans un message de contrôle d'accès ECM1. La condition d'accès CA2 et le cryptogramme de CW2 sont transportés dans un message de contrôle d'accès ECM2. La seule condition d'accès CA1 permet le désembrouillage du flux élémentaire, fournissant ainsi une image ou un son dégradé mais compréhensible pour l'usager.

On décrit maintenant comment précisément produire deux flux discernables, embrouillés respectivement avec les mots de contrôle CW1 et CW2, dans le cas d'un multiplex tramé et d'un multiplex en paquets.

Dans le cas du multiplex tramé tout d'abord, la composante sur laquelle on souhaite appliquer l'embrouillage progressif est transmise dans le canal i de chaque trame. Le procédé de l'invention consiste alors à embrouiller le canal i de m trames successives avec le mot CW1, puis le même canal de p trames successives avec CW2, puis à nouveau le même canal de m trames successives avec CW1, etc ... comme indiqué sur le schéma de la figure 4 où les traits verticaux symbolisent un embrouillage avec CW1 et les traits horizontaux un embrouillage avec CW2.

Les mots CW1 et CW2 changent de parité en même temps. Cette parité n'est pas indiquée sur le schéma de la figure 4.

Les valeurs des nombres m et p, propres à chacun des canaux embrouillés doivent être connues du décodeur de façon implicite ou explicite. Dans ce dernier cas, elles sont transmises dans la voie de service, accompagnées d'une information de synchronisation (par exemple une valeur particulière du compteur de trame) signalant à quelle trame commence l'embrouillage avec CW1 ou avec CW2.

A la réception le flux élémentaire est obtenu en désembrouillant les trames embrouillées avec CW1. Le flux complémentaire est obtenu en désembrouillant les trames embrouillées avec CW2. L'envoi au décodeur vidéo ou audio d'un seul flux élémentaire donne une image ou un son dégradé. L'envoi au décodeur vidéo ou audio du flux élémentaire accompagné du flux complémentaire donne une image ou un son de qualité.

La figure 5 montre, sur la première ligne, la composante embrouillée, sur la deuxième ligne la composante dégradée lorsque seul le flux élémentaire a été désembrouillé et, sur la troisième ligne, la composante complétement désembrouillée.

Le choix des nombres m et p doit être fixé en fonction des performances du décodeur vidéo ou audio et notamment en fonction de son temps d'accrochage. En règle générale, m est très supérieur à p car il faut très peu de trames embrouillées pour perturber fortement le comportement du décodeur vidéo ou audio.

Les moyens utilisés à l'émission sont représentés sur la figure 6. Ils comprennent un multiplexeur 20

avec une première sortie 21 délivrant les données en clair, une seconde sortie délivrant la synchronisation de trame, une troisième sortie délivrant les nombres m et p ainsi que le compteur de trame et la parité, et enfin une quatrième sortie 24 délivrant deux messages de contrôle d'accès ECM1, ECM2.

Les moyens comprennent encore un circuit 25 contenant les mots de contrôle utilisés (CW1 pair et impair et CW2 pair et impair) et l'embrouilleur 26 qui utilise l'un ou l'autre de ces mots. Ce circuit 25 délivre, sur une première sortie 27, les données embrouillées, sur une deuxième sortie 28, la synchronisation de trame, sur une troisième sortie 29, les nombres m, p ainsi que le compteur trame et la parité.

S'agissant maintenant du multiplex en paquets, le cas est proche de celui du multiplex en trames, la différence résidant dans la transmission des informations de synchronisation entre l'embrouilleur et le désembrouilleur. En effet, dans la cas du multiplex paquets, l'en-tête paquet peut être utilisé pour véhiculer l'information : c'est dans l'en-tête paquet que sera envoyée l'information d'embrouillage avec CW1 ou avec CW2, ainsi que la parité. Ceci permet, en particulier, à l'embrouilleur de faire varier les valeurs m et p.

Le nombre m peut, par exemple, correspondre au nombre de paquets nécessaire au codage d'une image intra tandis que le nombre p peut correspondre au nombre de paquets entre deux images intra.

On peut remarquer que l'embrouillage du flux élémentaire avec le mot de contrôle CW1 n'est pas obligatoire. Dans une variante simplifiée, on

n'embrouille pas le canal de rang i des groupes de m trames successives ; on n'embrouille que le canal de rang i des groupes de p trames successives et ceci avec le mot de contrôle CW2. On ne définit donc pas de conditions d'accès CA1 et on n'utilise pas le mot de contrôle CW1. Ceci revient à n'exercer aucun contrôle sur la réception du flux élémentaire et à offrir à tous les récepteurs l'accès à l'image ou au son dégradés.

On peut remarquer encore, comme plus haut, que le mot de contrôle CW1 peut être le mot de contrôle local connu du récepteur ou un mot de contrôle véhiculé à l'intérieur d'un message de contrôle d'accès.

La figure 7 montre comment l'on constitue le flux élémentaire avec des groupes de m paquets qui seront embrouillés avec le premier mot de contrôle CW1, et des groupes de p paquets qui seront embrouillés avec le second mot de contrôle CW2. Les traits verticaux symbolisent l'embrouillage avec CW1 et les traits horizontaux l'embrouillage avec CW2.

A la réception, le flux élementaire sera obtenu en désembrouillant les paquets embrouillés avec CW1. Le flux complémentaire sera obtenu en désembrouillant les paquets embrouillés avec CW2. L'envoi au décodeur vidéo ou audio d'un seul flux élémentaire donnera une image ou un son dégradé. L'envoi au décodeur vidéo ou audio du flux élémentaire accompagné du flux complémentaire donnera une image ou un son de qualité.

La figure 8 montre, sur la première ligne, la composante embrouillée, sur la deuxième ligne, la composante dégradée correspondant au seul flux élémentaire désembrouillé, et, sur la troisième ligne, la composante complétement désembrouillée (flux élementaire et flux complémentaire).

Là encore, le choix de m et de p doit être fixé en fonction des performances du décodeur vidéo ou audio et notamment en fonction de son temps d'accrochage. En règle générale, m sera très supérieur à p, car il faut très peu de paquets embrouillés pour perturber fortement le comportement du décodeur vidéo ou audio.

La figure 9 montre schématiquement les moyens utilisés à l'émission, dans la variante à multiplexage en paquets. Ces moyens comprennent un multiplexeur 30 qui délivre, sur une première sortie 31, les paquets en clair, sur une deuxième sortie 32, la synchronisation de paquets, sur une troisième sortie 33, les nombres m et p ainsi que la parité et sur une quatrième sortie 34, les messages de contrôle d'accès ECM1, ECM2.

Ces moyens comprennent encore un circuit 35 contenant les mots de contrôle CW1 pair et impair et les mots de contrôle CW2 pair et impair, et l'embrouilleur 36 utilisant ces mots. Le circuit 35 délivre, sur une première sortie 37, les paquets embrouillés et, sur une seconde sortie 38, un signal de parité.

Dans le multiplexage en paquets comme dans le multiplexage en trame, un cas particulier de mise en oeuvre du procédé consiste à ne pas définir de condition d'accès CA1 et à ne pas utiliser le mot de contrôle CW1. Ceci revient à n'exercer aucun contrôle sur la réception du flux élementaire et à offrir à tous les récepteurs l'accès à l'image ou au son dégradés. On peut aussi utiliser, comme mot de contrôle CW1, le mot de contrôle local connu du récepteur ou un mot de contrôle véhiculé à l'intérieur d'un message de contrôle d'accès.

Pour finir, on peut préciser un mode de mise en oeuvre du procédé de l'invention dans le cas du multiplexage dit MPEG2.

Dans le cas particulier de MPEG2, la signalisation propre à l'embrouillage dans l'en-tête de chaque paquet est constituée de deux bits appelés "Transport-Scrambling-Control" (TSC) dans le projet de norme MPEG2 Système (ISO/IEC CD 13818-1). Les valeurs de ces deux bits sont actuellement normalisées :

00 : le paquet n'est pas embrouillé

01 : est réservé

10 : le paquet est embrouillé avec le mot de contrôle pair

11 : le paquet est embrouillé avec le mot de contrôle impair.

Afin de mettre en oeuvre le procédé décrit ci-dessus, il faut pouvoir signaler au décodeur non plus deux mots de contrôle (pair ou impair), mais en tout, quatre mots de contrôle (CW1 pair, CW2 pair, CW1 impair, CW2 impair). Il faut pouvoir indiquer lequel de ces quatre mots de contrôle a été utilisé pour embrouiller le champ de données du paquet. Pour cela, on peut utiliser la valeur "01" aujourd'hui réservée.

Le comportement du décodeur est alors le suivant (le comportement du codeur s'en déduit aisément). On suppose que le décodeur dispose d'une mémoire de parité (1 bit suffit) baptisée MEM-PAR :

- Etat initial : MEM-PAR=0 ou 1
- Réception d'un paquet avec TSC="00" :
  aucune action de désembrouillage n'est à entreprendre
- Réception d'un paquet avec TSC="10" :

désembrouillage du paquet avec CW2 pair et MEM-PAR→0 (c'est-à-dire stocker la valeur "0" dans MEM-PAR)

- Réception d'un paquet avec TSC="11" :
  désembrouillage du paquet avec CW2 impair et MEM-PAR→1 (c'est-à-dire stocker la valeur "1" dans MEM-PAR)
- Réception d'un paquet avec TSC="01" :
  désembrouillage du paquet avec CW1 pair si MEM-PAR=0 ou avec CW1 impair si MEM-PAR=1.

Au branchement du récepteur, le contenu de la mémoire de parité MEM-PAR a une probabilité 1/2 d'être erroné jusqu'à réception du premier paquet avec TSC="10" ou "11". Le temps d'attente maximum avant d'être parfaitement synchronisé est de m paquets. Il est donc nécessaire, dans la mise en oeuvre de cette variante, de s'assurer que ce délai n'est pas perceptible pour l'utilisateur (valeur de m la plus faible possible).

On remarquera que le cas particulier de mise en oeuvre du procédé consistant à ne pas définir de condition d'accès CA1 et à ne pas utiliser le mot de contrôle CW1 est facilement réalisable en utilisant la valeur TSC="00" au lieu de TSC="01".

Le décodeur ayant uniquement accès à l'image dégradée peut fonctionner selon plusieurs modes :
- envoyer au décodeur vidéo les images désembrouillées ainsi que les images restant embrouillées,
- envoyer au décodeur vidéo uniquement les images désembrouillées, et le décodeur vidéo gèle la dernière image reçue pendant la réception des images embrouillées.

La figure 10 illustre schématiquement un récepteur apte à recevoir les programmes émis selon le procédé qui a été décrit. Sur cette figure, le récepteur porte la référence générale 40. Ce récepteur comprend une entrée générale 41, un démodulateur 42, un démultiplexeur-désembrouilleur 44, un processeur de sécurité 46, un décodeur vidéo 48, un décodeur audio 50, un décodeur de données 52, un écran d'affichage 54, un haut-parleur 56 et un ordinateur personnel 58.

Le signal reçu sur l'entrée 41 est d'abord démodulé dans le circuit 42 puis envoyé au démultiplexeur/désembrouilleur 44 qui extrait les trames ou paquets de la composante sélectionnée et les désembrouille si l'usager dispose des droits d'accès requis.

Le signal est ensuite envoyé au décodeur vidéo 48 s'il s'agit d'un signal vidéo, au décodeur audio 50 s'il s'agit d'un signal audio, ou au décodeur de données 52 s'il s'agit d'un signal de données. Une fois le signal décodé, il est présenté à l'usager sur le support adapté : écran 54 pour la vidéo, haut-parleur 56 pour audio et ordinateur 58 pour les données.

Dans le cas d'un multiplex tramé, le demultiplexeur-désembrouilleur 44 est organisé selon la figure 11.

L'entrée générale E est reliée à un démultiplexeur de trame 60 possédant trois sorties, respectivement 61 pour les données embrouillées 62, pour la synchronisation de trame et 63 pour les nombres m et p, le compteur de trame et la parité.

Le désembrouilleur 64 reçoit soit les mots de contrôle pair CW1 ou CW2, soit les mots de contrôle impairs CW1, CW2 selon la parité et désembrouille les

signaux. Les signaux en clair sont disponibles sur la sortie S.

Le démultiplexeur/désembrouilleur analyse la voie de service pour y récupérer (s'il ne les connaît pas de manière implicite) les valeurs de m, de p ainsi que l'information de synchronisation signalant à quelle trame commence l'embrouillage avec CW1 ou avec CW2.

Le démultiplexeur/désembrouilleur récupère les ECM1 et les ECM2 . Il envoie ces ECM au processeur de sécurité du décodeur (souvent une carte à microprocesseur) pour vérifications des conditions d'accès CA1 et CA2 et calcul des mots de contrôle CW1 et CW2 si les conditions d'accès sont respectées.

Si l'usager ne satisfait ni CA1 ni CA2, la composante reste entièrement embrouillée.

Si l'usager satisfait la condition d'accès CA1, mais pas la condition d'accès CA2, il a accès à une image ou un son ou des données dégradées. Le démultiplexeur/désembrouilleur désembrouille les salves de m trames embrouillées avec CW1. Il engendre ainsi un flux constitué de m trames en clair, puis p trames embrouillées, puis à nouveau m trames en clair, etc... Ce flux est envoyé au décodeur vidéo ou audio ou de données.

Si la composante est une composante audio, le décodeur audio peut tout décoder (le décodage des trames embrouillées se traduira par du bruit sur le haut-parleur) ou peut décider de ne pas décoder les salves de p trames restant embrouillées (pas de son sur le haut-parleur pendant le passage de ces trames).

Si la composante est une composante vidéo, le décodeur vidéo peut tout décoder (le décodage des trames embrouillées se traduira par une image bruitée sur l'écran) ou peut décider de ne pas décoder les

salves de p trames restant embrouillées et de geler sur l'écran pendant ce temps la dernière image correctement décodée.

Si l'usager satisfait les conditions d'accès CA1 et CA2, il a accès à une image ou un son ou des données complétement désembrouillées.

Le démultiplexeur/désembrouilleur désembrouille les salves de trames embrouillées avec CW1 et les salves de p trames embrouillées avec CW2. Il engendre ainsi un flux constitué de trames complètement désembrouillées. Ce flux est envoyé au décodeur vidéo ou audio ou données.

Un cas particulier consiste à ne pas définir de condition d'accès CA1 et à ne pas utiliser le mot de contrôle CW1 (les salves de m trames sont en clair). Ceci revient à n'exercer aucun contrôle sur la réception du flux élémentaire et à offrir à tous les récepteurs l'accès à l'image ou au son dégradé.

Dans le cas d'un multiplex par paquets, le démultiplexeur-désembrouilleur 44 est organisé selon la figure 12. L'entrée E' est reliée à un démultiplexeur de paquets 60' possédant trois sorties, respectivement 61' délivrant les paquets embrouillés, 62' pour la synchronisation de paquets et 63' pour les nombres m et p et pour la parité.

Le désembrouilleur 64' reçoit soit les mots de contrôle pair CW1 ou CW2, soit les mots de contrôle impairs CW1, CW2, selon la parité, et désembrouille les signaux. Les signaux en clair sont disponibles sur la sortie S'.

Le démultiplexeur/désembrouilleur récupère les ECM1 et les ECM2. Il envoie ces ECM au processeur de

sécurité du décodeur (souvent une carte à microprocesseur) pour vérifications des conditions d'accès CA1 et CA2 et calcul des mots de contrôle CW1 et CW2 si les conditions d'accès sont respectées.

Si l'usager ne satisfait ni CA1, ni CA2, la composante reste entièrement embrouillée.

Le démultiplexeur/désembrouilleur analyse l'entête des paquets pour savoir avec quel CW il faut désembrouiller le paquet (CW1 pair, CW1 impair, CW2 pair, CW2 impair).

Si l'usager satisfait la condition d'accès CA1, mais pas la condition d'accès CA2, il a accès à une image ou son ou données dégradé selon le mécanisme ci-dessous.

Le démultiplexeur/désembrouilleur désembrouille les salves de m paquets embrouillés avec CW1. Il engendre ainsi un flux constitué de m paquets en clair, puis p paquets embrouillés, puis à nouveau m paquets en clair, etc... Ce flux est envoyé au décodeur vidéo ou audio ou de données.

Si la composante est une composante audio, le décodeur audio peut tout décoder (le décodage des paquets embrouillés se traduira par du bruit sur le haut-parleur) ou peut décider de ne pas décoder les salves de p paquets restant embrouillés (pas de son sur le haut-parleur pendant le passage de ces paquets).

Si la composante est une composante vidéo, le décodeur vidéo peut tout décoder (le décodage des paquets embrouillés se traduira par une image bruitée sur l'écran) ou peut décider de ne pas décoder les salves de p paquets restant embrouillés et de geler sur l'écran pendant ce temps la dernière image correctement décodée.

Si l'usager satisfait les conditions d'accès CA1 et CA2, il a accès à une image ou un son ou des données complètement désembrouillés.

Le démultiplexeur/désembrouilleur désembrouille les salves de paquets embrouillées avec CW1 et les salves de paquets embrouillées avec CW2. Il engendre ainsi un flux constitué de paquets complètement désembrouillés. Ce flux est envoyé au décodeur vidéo ou audio ou données.

Un cas particulier de mise en oeuvre consiste à ne pas définir de condition d'accès CA1 et à ne pas utiliser le mot de contrôle CW1 (les salves de m paquets sont en clair). Ceci revient à n'exercer aucun contrôle sur la réception du flux élémentaire et à offrir à tous les récepteurs l'accès à l'image ou au son dégradés.

REVENDICATIONS

1. Procédé de diffusion de programmes à accès conditionnel progressif, dans lequel :

- on sépare un flux d'information corespondant à une composante d'un programme en un premier flux, dit flux élémentaire et en un second flux, dit flux complémentaire,
- on embrouille au moins le flux complémentaire à l'aide d'un mot de contrôle (CW2),
- de manière synchrone avec chaque programme, on transmet des messages de contrôle d'accès (ECM) permettant de désembrouiller et de restituer les flux embrouillés dans des récepteurs disposant des droits d'accès correspondants, la restitution du seul flux élémentaire conduisant à une composante de programme discernable sans être directement utilisable, le désembrouillage du flux complémentaire permettant de compléter la composante du programme pour permettre de restituer complétement le programme,

ce procédé étant caractérisé par le fait que, le flux d'information étant sous forme de multiplex numérique constitué d'une suite d'éléments, on constitue le flux élémentaire en prenant, dans le multiplex, des groupes de m éléments successifs et on constitue le flux complémentaire en prenant, dans le multiplex, des groupes de p éléments successifs, les groupes de m éléments successifs alternant avec les groupes de p éléments successifs.

2. Procédé selon la revendication 1, caractérisé par le fait que les éléments du multiplex sont des trames de longueur fixe, découpées en canaux de longueur variable, la composante du programme à

embrouiller étant transmise dans un canal de rang déterminé et par le fait qu'on constitue le flux élémentaire en prenant les informations contenues dans le canal ayant ce rang déterminé (i) dans les groupes de m trames successives et le flux complémentaire par les informations contenues dans le canal de même rang déterminé (i) dans des groupes de p trames successives alternant avec lesdits groupes de m trames successives.

3. Procédé selon la revendication 2, caractérisé par le fait qu'on embrouille le canal de rang déterminé (i) des groupes de m trames successives par un premier mot de contrôle (CW1) et le canal de même rang (i) des groupes de p trames successives par un second mot de contrôle (CW2).

4. Procédé selon la revendication 3, caractérisé par le fait que le premier mot de contrôle (CW1) est un mot de contrôle connu du récepteur ou véhiculé à l'intérieur d'un message de contrôle d'accès.

5. Procédé selon la revendication 2, caractérisé par le fait qu'on n'embrouille pas le canal de rang déterminé (i) des groupes de m trames successives mais qu'on embrouille le canal de rang déterminé (i) des groupes de p trames successives par un mot de contrôle (CW2).

6. Procédé selon l'une quelconque des revendications 3 ou 5, caractérisé par le fait que l'on transmet, avec les messages de contrôle d'accès, la valeur des nombres m et p, ainsi qu'une information indiquant à partir de quelle trame commence l'embrouillage avec le premier ou le second mot de contrôle (CW1, CW2).

7. Procédé selon la revendication 1, caractérisé par le fait que les éléments du multiplex sont des paquets et qu'on constitue le flux élémentaire par les informations contenues dans des groupes de m paquets successifs et le flux complémentaire par les informations contenues dans les groupes de p paquets successifs alternant avec les groupes de m paquets successifs.

8. Procédé selon la revendication 7, caractérisé par le fait qu'on embrouille les paquets des groupes de m paquets successifs par un premier mot de contrôle (CW1) et les paquets des groupes de p paquets successifs par un second mot de contrôle (CW2).

9. Procédé selon la revendication 8, caractérisé par le fait que le premier mot de contrôle (CW1) est un mot de contrôle connu du récepteur ou véhiculé à l'intérieur d'un message de contrôle d'accès.

10. Procédé selon la revendication 7, caractérisé par le fait qu'on n'embrouille pas les paquets des groupes de m paquets successifs mais qu'on embrouille les paquets des groupes de p paquets successifs par un mot de contrôle (CW2).

11. Procédé selon l'une quelconque des revendications 8 ou 10, caractérisé par le fait que, chaque paquet comprenant un en-tête, on transmet une information relative au mot de contrôle utilisé (CW1, CW2) dans l'en-tête de paquet.

12. Procédé selon la revendication 7, caractérisé par le fait que les couches m et p sont variables.

13. Procédé selon la revendication 3 ou selon la revendication 8, caractérisé par le fait que :

- chaque mot de contrôle utilisé (CW1, CW2) possède une durée de vie limitée à une période de temps appelée phase, les phases successives étant alternativement paires et impaires, le message de contrôle d'accès (EMC1, EMC2) relatif à un mot de contrôle (CW1, CW2) comprenant à la fois le mot de contrôle courant de la phase courante et le mot de contrôle futur de la phase suivante, l'un étant appelé mot pair (CW_e) et étant utilisé pendant une phase paire, l'autre étant appelé mot impair (CW_0) et étant utilisé pendant une phase impaire,
- les premier et second mots de contrôle (CW1, CW2) changent de parité en même temps,
- quatre mots de contrôle sont mis en oeuvre, à savoir les mots pair et impair ($CW1_e$, $CW1_0$) relatifs au premier mot de contrôle (CW1) et les mots pair et impair ($CW2_e$, $CW2_0$) relatifs au second mot de contrôle (CW2),
- on transmet une information de parité relative aux mots de contrôle utilisés.

14) Récepteur destiné à recevoir des programmes à accès conditionnel progressif émis selon le procédé de la revendication 1, caractérisé par le fait qu'il comprend :

- des moyens (60, 60') pour séparer dans le flux d'information reçu un premier flux, dit flux élémentaire, constitué par des groupes de m éléments successifs, et un second flux, dit flux complémentaire, constitué par des groupes de p éléments successifs, les groupes de m éléments

successifs alternant avec les groupes de p éléments successifs,

- des moyens (46) pour reconnaître au moins un message de contrôle d'accès (ECM) dans les informations reçues et pour en extraire au moins un mot de contrôle (CW) et au moins une condition d'accès (CA),
- des moyens (46) pour vérifier si au moins ladite condition d'accès (CA) est satisfaite,
- des moyens (64, 64') pour désembrouiller au moins le flux complémentaire à l'aide du mot de contrôle associé (CW2), si la condition d'accès correspondante (CA2) est satisfaite,
- au moins un récepteur vidéo (54) audio (56) ou de données (58) recevant au moins les signaux du flux élémentaire et, le cas échéant, les signaux du flux complémentaire désembrouillé si la condition d'accès correspondante est satisfaite.

15. Récepteur selon la revendication 14, caractérisé par le fait que :

- les moyens (46) pour reconnaître les messages de contrôle d'accès (ECM) sont aptes à reconnaître deux messages de contrôle d'accès (ECM1, ECM2) et à restituer deux mots de contrôle (CW1, CW2) et deux conditions d'accès (CA1, CA2),
- les moyens (46) pour vérifier si au moins une condition d'accès est satisfaite sont aptes à vérifier si les deux conditions d'accès (CA1, CA2) sont satisfaites,
- les moyens (64, 64') pour désembrouiller au moins le flux complémentaire à l'aide du second mot de contrôle (CW2) sont aptes en outre à désembrouiller le flux élémentaire à l'aide du premier mot de contrôle (CW1).

16. Récepteur selon la revendication 14, caractérisé par le fait que :

- les moyens (46) pour reconnaître au moins un message de contrôle d'accès (ECM) sont aptes à reconnaître un seul message de contrôle d'accès (ECM2) et à restituer un seul mot de contrôle (CW2) et une seule condition d'accès (CA2),
- les moyens (46) pour vérifier si au moins une condition d'accès est satisfaite vérifie seulement si ladite condition (CA2) est satisfaite,
- les moyens (64, 64') pour désembrouiller au moins le flux complémentaire désembrouille uniquement ledit flux à l'aide du seul mot de contrôle restitué (CW2).

17. Récepteur selon la revendication 16, caractérisé par le fait que les moyens (64, 64') pour désembrouiller au moins le flux complémentaire sont aptes en outre à désembrouiller le flux élémentaire à l'aide d'un mot de contrôle connu du récepteur.

18. Récepteur selon la revendication 14, caractérisé par le fait que les moyens (46) aptes à reconnaître au moins un message de contrôle d'accès sont aptes à extraire quatre mots de contrôle, à savoir : des premier et second mots pairs (CW1 pair, CW2 pair) et des premier et second mots impairs (CW1 impair, CW2 impair), le récepteur comprenant en outre une mémoire de parité à au moins un bit (MEM-PAR) et un moyen de reconnaissance de l'état d'un groupe de deux bits reçus (TSC).

19. Récepteur selon l'une quelconque des revendications 14 à 18, caractérisé par le fait que les récepteurs vidéo (54), audio (56) ou de données (58) reçoivent reçoit à la fois les signaux désembrouillés et les signaux embrouillés.

20. Récepteur selon l'une quelconque des revendications 14 à 18, caractérisé par le fait que les récepteurs vidéo (54), audio (56) ou de données (58) ne reçoivent que les signaux désembrouillés.

WO 95/28058 PCT/FR95/00435

FIG. 1

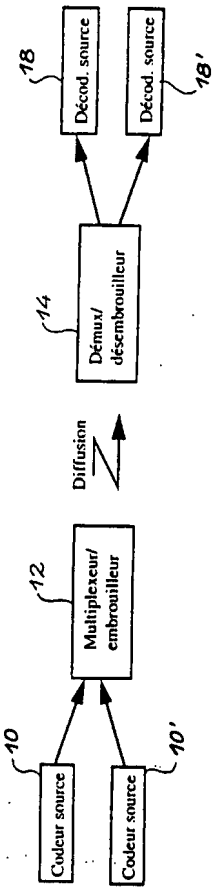


FIG. 2

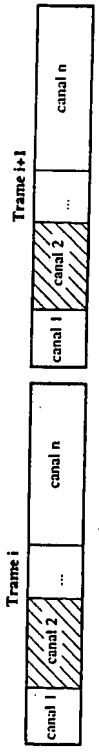
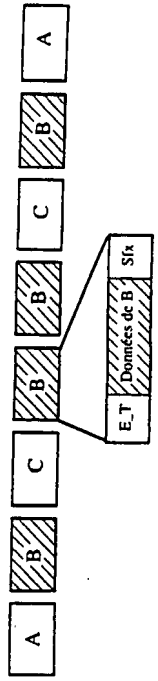


FIG. 3



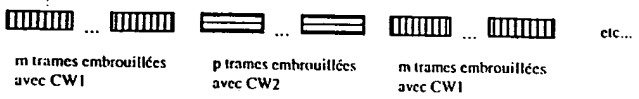


FIG. 4

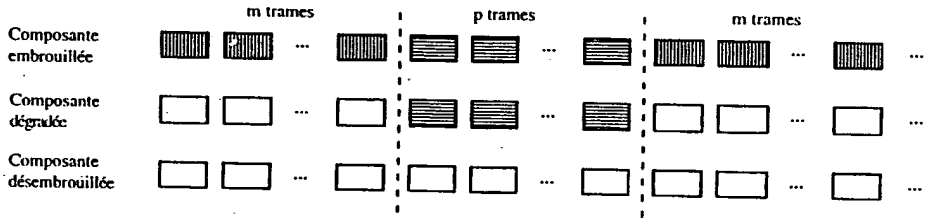


FIG. 5

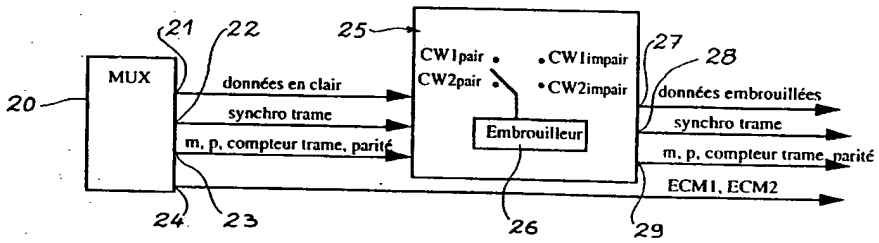


FIG. 6

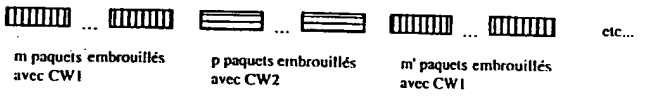


FIG. 7

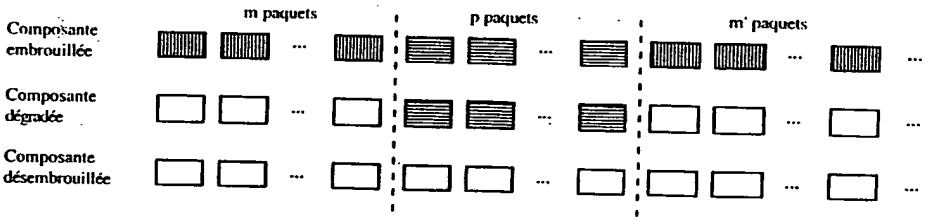


FIG. 8

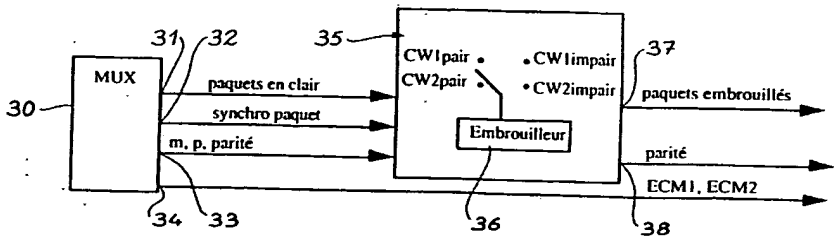


FIG. 9

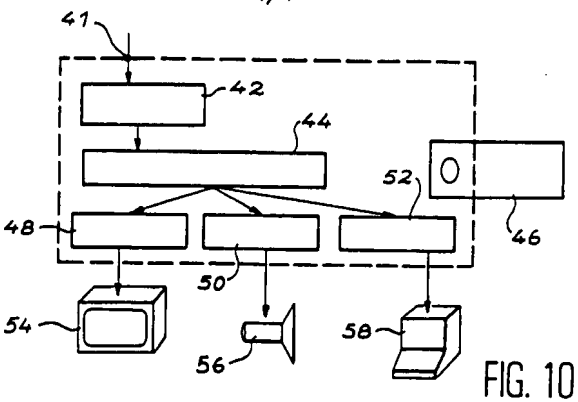


FIG. 10

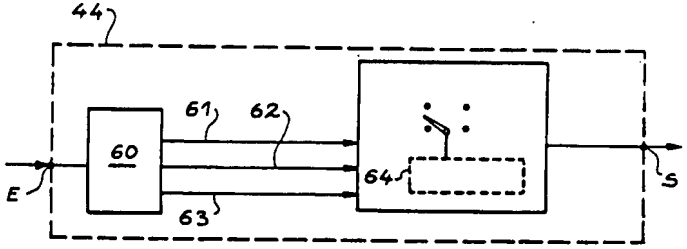


FIG. 11

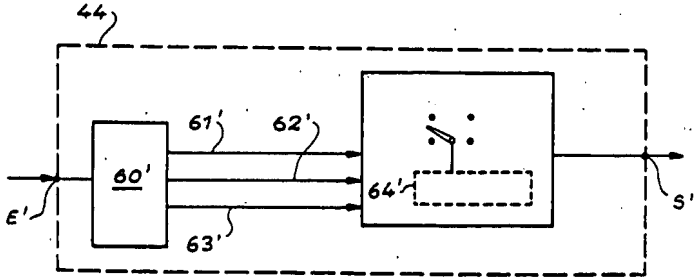


FIG. 12

INTERNATIONAL SEARCH REPORT

Interna ..al Application No
PCT/FR 95/00435

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	18TH INTERNATIONAL TELEVISION SYMPOSIUM AND TECHNICAL EXHIBITION, 15 June 1993 MONTREUX, SWITZERLAND, pages 761-769, VIGARI 'A DEVICE FOR REAL-TIME MODIFICATION OF ACCESS CONDITIONS IN A D2-MAC/PACKET EUROCRYPT SIGNAL : THE TRANSCONTROLLER'	1
A	see the whole document ---	2-20
Y	IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, vol. 38, no. 3, August 1992 NEW YORK, US, pages 188-194, ANGEBAUD ET AL. 'CONDITIONAL ACCESS MECHANISMS FOR ALL-DIGITAL BROADCAST SIGNALS'	1
A	see the whole document --- -/--	2-20

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents :

'A' document defining the general state of the art which is not considered to be of particular relevance

'E' earlier document but published on or after the international filing date

'L' document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

'O' document referring to an oral disclosure, use, exhibition or other means

'P' document published prior to the international filing date but later than the priority date claimed

'T' later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

'X' document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

'Y' document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

'&' document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 July 1995	25.07.95

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	Greve, M

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Intern ..al Application No
PCT/FR 95/00435

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP-A-0 461 029 (MATRA COMMUNICATION) 11 December 1991 see the whole document ---	1-20
A	EP-A-0 583 202 (FRANCE TELECOM) 16 February 1994 see page 3, line 48 - page 5, line 4 -----	1-20

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern ..al Application No
PCT/FR 95/00435

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP-A-0461029	11-12-91	FR-A-	2663179	13-12-91
		AU-B-	636039	08-04-93
		AU-A-	7828591	12-12-91
		DE-D-	69108781	18-05-95
		JP-A-	4233345	21-08-92
EP-A-0583202	16-02-94	FR-A-	2694860	18-02-94
		CA-A-	2103935	14-02-94
		US-A-	5349641	20-09-94

Form PCT/ISA/210 (patent family annex) (July 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 95/00435

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 H04N7/167

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 6 H04N

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	18TH INTERNATIONAL TELEVISION SYMPOSIUM AND TECHNICAL EXHIBITION, 15 Juin 1993 MONTREUX, SWITZERLAND, pages 761-769, VIGARI 'A DEVICE FOR REAL-TIME MODIFICATION OF ACCESS CONDITIONS IN A D2-MAC/PACKET EUROCRYPT SIGNAL : THE TRANSCONTROLLER'	1
A	voir le document en entier	2-20
Y	IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, vol. 38, no. 3, Août 1992 NEW YORK, US, pages 188-194, ANGEBAUD ET AL. 'CONDITIONAL ACCESS MECHANISMS FOR ALL-DIGITAL BROADCAST SIGNALS'	1
A	voir le document en entier	2-20

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
10 Juillet 1995	25.07.95

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tél. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+ 31-70) 340-3016	Greve, M

Formulaire PCT/ISA 210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 95/00435

C(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP-A-0 461 029 (MATRA COMMUNICATION) 11 Décembre 1991 voir le document en entier	1-20
A	EP-A-0 583 202 (FRANCE TELECOM) 16 Février 1994 voir page 3, ligne 48 - page 5, ligne 4	1-20

Formulaire PCT/ISA 210 (suite de la deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 95/00435

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP-A-0461029	11-12-91	FR-A-	2663179	13-12-91
		AU-B-	636039	08-04-93
		AU-A-	7828591	12-12-91
		DE-D-	69108781	18-05-95
		JP-A-	4233345	21-08-92
EP-A-0583202	16-02-94	FR-A-	2694860	18-02-94
		CA-A-	2103935	14-02-94
		US-A-	5349641	20-09-94